



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

Address: COMMISSIONER FOR PATENTS

P.O. Box 1450

Alexandria, Virginia 22313-1450

www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/734,935	12/12/2003	Michel S. Simpson	26530.92	2224
27683	7590	02/03/2011		
HAYNES AND BOONE, LLP				
IP Section				
2323 Victory Avenue				
Suite 700				
Dallas, TX 75219				
EXAMINER				
LEMMA, SAMSON B				
ART UNIT		PAPER NUMBER		
2432				
MAIL DATE		DELIVERY MODE		
02/03/2011		PAPER		

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

# Office Action Summary

**Application No.**

10/734,935

**Applicant(s)**

SIMPSON ET AL.

**Examiner**

SAMSON LEMMA

**Art Unit**

2432

**Period for Reply** -- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on RCE filed on 12 July 2010.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1 and 4-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1 and 4-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftperson's Patent Drawing Review (PTO-945)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

### *DETAILED ACTION*

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 07/12/2010 has been entered. Claims 2,3 are canceled and claims 1, 4-21 are pending of which claims 1, 11 and 21 are independent. All independent claims are amended.
2. The 112 first paragraph rejection set forth in the previous office action is overcome and withdrawn.
3. The 101 rejection set forth in the previous office action is overcome and withdrawn.

### ***Priority***

4. This application does not claim priority. Therefore, the effective filing data for the subject matter defined in the pending claims of this application is **12/12/2003**.

### *Response to Arguments*

5. Applicant's remark/arguments filed on 07/12/2010 have been fully considered but they are not persuasive.

The argument presented that the art on the record does not disclose the following new limitation added in each independent claim is not found to be persuasive,  
“denying access to the second data portion in accordance with the access right, wherein the denying access comprises at least one of logging information regarding the denial of access of access to the second data portion, and notifying security personnel regarding the denial of access to the second data portion”

A close review of the reference on the record namely Carter on column 16, lines 38-50 discloses the following which meets the above limitations.  
*“Accordingly, the collaborative access controller 44 performs a limiting step 156 to limit access to the information in the data portion 94 of the work group document 90. In one embodiment, the limiting step merely denies the user access by preventing decryption of the data portion 94. In other embodiments, decryption is prevented and additional steps are taken as well. One embodiment logs information about the failed attempt, such as the time, workstation, collaborative document name, user identifier, etc. Another embodiment uses e-mail, telephony, alarms, or other conventional means to notify security personnel of the failed attempt. A third embodiment both logs the information and notifies security.”*

Applicant's other remark/arguments filed on 07/12/2010 **regarding the ACL have been fully considered but are moot in view of new ground(s) of rejection.**

Examiner Note: Please see also the cited reference at the end of this office action regarding the ACL limitation recited at least in independent claim

1.

### ***Claim Rejections - 35 USC § 103***

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. **Claims 1, 4-10** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stephen R. Carter** (hereinafter referred as **Carter**) (U.S. Patent No. 5,787,175) (Date of patent 28, 1998), in view of **Rider** (hereinafter referred to as **Rider**) (U.S. Patent Publication 2006/0173999 A1) (filed on 08/07/2003, claims priority of a provisional application filed on 08/07/2002) further in view Koyama et al (hereinafter referred as **Koyama**) (U.S. Patent No. 7,191,195 B2, filed on Nov 27, 2002)

8. **As per independent claim 1 Carter discloses a method for controlling access to a document, [Abstract] comprising:**

- **Determining an access right for a user; (Column 12, lines 56-63; column 15, lines 62-67; abstract and column 8, lines 27-29)**

*(Access control Methods FIGS. 4-9 illustrate one method according to the present invention for controlling collaborative access to the work group document 90. In particular, the method includes computer-implemented steps for collaboratively encrypting the document 90 (FIG. 6) and steps for restricting access to the data portion 94 of the collaboratively encrypted document (FIG. 9)).*

- **building a member definition [Figure 5, see "member definition"] comprising a member identifier [Figure 5, ref. Num "98", See "member identifier"], an access control [See column 12, lines 56-57; column 13, lines 52-62, see figure 5, ref. Num 100, "encrypted document key" signed by the public key of the member. Only the member with the corresponding private key can access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public**

key 78 used to encrypt the document-key. "See also "collaborative access controller 44" which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted from accessing the information. See for instance the following disclosed on column 6, lines 11-12, "users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"] **a private key of a key pair for use in encrypting the document** [column 14 lines 16-22 and column 14, lines 4-5] ("As noted, the member definition 96 includes the encrypted message digest 102 if the member in question has collaboratively signed the document 90. As explained in greater detail below in connection with FIG. 10, the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and **then encrypting that message digest with the private key 80 of the member who is signing the document 90.**" Furthermore on column 14, lines 4-5, it has also been disclosed that the private key 80 is a key pair which corresponds to the public key 78. Thus, the message digest 102 which is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90 implicitly contains the private key of the member who is signing the document. With out the private key, it is not possible to produce the said message digest. Furthermore as it is disclosed on column 14, lines 4-5, the private key 80 is a key pair which corresponds to the public key 78 and

*this meets the argued limitation, “building a member definition comprising, a private key of a key pair for use in encrypting the document”)*

**and a digital signature,***[See also figure 5, ref. Num “102”, “encrypted message digest”, signed by the private key. In particular see what is disclosed on column 14, lines 15-21, “the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90.” See also the abstract and column 6, lines 11-12, “collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member.”] and associating the member definition with the user. [Figure 5 and column 6, lines 11-22, See “Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot”]*

and

- **Linking the member definition to a portion of a document.**

*[Figure 6, ref. Num “120” (“Link member definition(s) with document.”)]*

- **denying access to the second data portion in accordance with the access right, wherein the denying access comprises at least one of logging information regarding the denial of access of access to**



**the second data portion, and notifying security personnel regarding the denial of access to the second data portion**[Column 16, lines 38-50] (*"Accordingly, the collaborative access controller 44 performs a limiting step 156 to limit access to the information in the data portion 94 of the work group document 90. In one embodiment, the limiting step merely denies the user access by preventing decryption of the data portion 94. In other embodiments, decryption is prevented and additional steps are taken as well. One embodiment logs information about the failed attempt, such as the time, workstation, collaborative document name, user identifier, etc. Another embodiment uses e-mail, telephony, alarms, or other conventional means to notify security personnel of the failed attempt. A third embodiment both logs the information and notifies security."*)

**Carter** does not explicitly disclose

linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion, receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right

However, in the same field of endeavor, **Rider** discloses,

**Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion**, [paragraph 0044, figure 4A & 0034-0035] (As

*shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is, **one or more access rights can be associated with portion 406**. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)*

**Receiving a request from the user to access the document;  
comparing the request with the access right; and allowing access to  
only the first data portion in accordance with the access right**

[Paragraph 0034-0035 paragraph 0044, figure 4A] *(On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user **request to access one or more documents** as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource, **a particular document or only a portion of a document**. Furthermore on paragraph 0035, the following has been disclosed. "By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is realized. Hence, tier two security restricts a user to data **constituting a portion of an entire document rather than***

***providing complete or no access to that document. For example, FIG. 4A depicts document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.***")

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion and receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right as per teachings of **Rider** into the method as taught by **Carter**, in order to provide a more fine-grained access control to the resources (portions of documents) [See *For instance Rider on paragraph 0035*]

**The combination of Carter and Rider does** not explicitly disclose that the access control is actually the "access control list"

However, in the same field of endeavor **Koyama at least on column 7 and figure 9 discloses the "access control list"**

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to employ features such as access control as per teachings of **Koyama** into the method of "access control" as taught by the combination of **Carter and Rider**, in order to enhance the

security by providing further fine-grained access control to the resources)

[See For instance Frey column 4, lines 35-40 ]

9. **As per dependent claim 4 the combination of Carter, Rider and Koyama** discloses a method as applied to claims above.  
Furthermore, Carter discloses the method, further comprising adding a new user to the document. [Figure 7, column 7, lines 3-5] (“adding a new member”)
10. **As per dependent claim 5 the combination of Carter, Rider and Koyama** discloses a method as applied to claims above.  
Furthermore, Carter discloses the method, further comprising removing a member from the document. [Figure 8, column 7, lines 5-7] (“removing a member”)
11. **As per dependent claim 6 the combination of Carter, Rider and Koyama** discloses a method as applied to claims above.  
Furthermore, Carter discloses the method further comprising: storing the member definition remotely from the document. [column 14, lines 35-38]
12. **As per dependent claim 7 the combination of Carter, Rider and Koyama** discloses a method as applied to claims above.  
Furthermore, Carter discloses the method further comprising: storing the member definition in the document. [Column 14, lines 31-34] ( “In one embodiment, linking is accomplished by storing the encrypted

*data portion 94 and the prefix portion 92 (including one or more **member definitions** 96) together in a file on a disk, tape, or other conventional **storage** medium.”)*

13. **As per dependent claim 8 the combination of Carter, Frey and Koyama** discloses a method as applied to claims above.

**Furthermore, Carter discloses the method further comprising:  
further comprising:**

**encrypting the document; and linking the member definition with a public key and a private key.**[column 11, lines 61- column 12, lines 7]

14. **As per claims 9-10 the combination of Carter, Rider and Koyama**

discloses a method as applied to claims above. Furthermore, Rider discloses the method, further comprising: determining a second access right for the user; building a second member definition using the second access right; and linking the second member definition to a second portion of a document [Paragraph 0034-0035 paragraph 0044, figure 4A].

15. **Claims 11-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Stephen R. Carter** (hereinafter referred as **Carter**)(U.S. Patent No. 5,787,175) (Date of patent 28, 1998), in view of **Rider** (hereinafter referred to as **Rider**) (U.S. Patent Publication 2006/0173999 A1) (filed on 08/07/2003, claims priority of a provisional application filed on 08/07/2002)

16. **As per independent claim 11 Carter discloses a computer implemented system for controlling access to a document comprising a microprocessor, a memory accessible by the microprocessor, [Abstract] comprising:**

- **A document comprising a first data and a second data.**[  
*“the documents, which are indicated as 4, ref. Num “92” could be more than one as it is indicated on column 14, lines 23-24 and figure 4-6, the system builds one or more member definitions which is associated with one or more documents.]*  
  
**a first member definition** [figure 5, ref. Num “96”, “Member definition “] **associated with the first data**[See figure 4, ref. Num “92”/”document “] **wherein the first member definition contains a first user identifier** [Figure 5, ref. Num “98”] **and a private key of a key pair for use in encrypting the document** [column 14 lines 16-22 and column 14, lines 4-5] (*“As noted, the member definition 96 includes the encrypted message digest 102 if the member in question has collaboratively signed the document 90. As explained in greater detail below in connection with FIG. 10, the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90.”*  
*Furthermore on column 14, lines 4-5, it has also been disclosed that the private key 80 is a key pair which corresponds to the public key 78. Thus,*

*the message digest 102 which is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90 implicitly contains the private key of the member who is signing the document. With out the private key, it is not possible to produce the said message digest. Furthermore as it is disclosed on column 14, lines 4-5, the private key 80 is a key pair which corresponds to the public key 78 and this meets the argued limitation, "building a member definition comprising, a private key of a key pair for use in encrypting the document")*

**a first access right for a first user for the first data** [Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key."];

**As it is indicated 14, lines 23-24 and figure 4-6, the system builds one or more member definitions. And the member definitions shown on figure 5, is associated to the documents shown on figure 4. Even though only one document is shown on figure 4, ref. Num "54, 90" the system is built for one or more documents. See the documents described on column 9, lines 35.**

**Thus the following is also correct.**

**a second member definition** [figure 5, ref. Num "96", "Member definition "] **associated with the second data** [See figure 4, ref. Num "92"/"document "], **wherein the second member definition contains a second user identifier**[Figure 5, ref. Num "98"] **and a private key of a second key pair for use in encrypting the second data** [column 14 lines 16-22 and column 14, lines 4-5] (*"As noted, the member definition 96 includes the encrypted message digest 102 if the member in question has collaboratively signed the document 90. As explained in greater detail below in connection with FIG. 10, the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90."* Furthermore on column 14, lines 4-5, it has also been disclosed that the private key 80 is a key pair which corresponds to the public key 78. Thus, the message digest 102 which is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message



*digest with the private key 80 of the member who is signing the document 90 implicitly contains the private key of the member who is signing the document. With out the private key, it is not possible to produce the said message digest. Furthermore as it is disclosed on column 14, lines 4-5, the private key 80 is a key pair which corresponds to the public key 78 and this meets the argued limitation, "building a member definition comprising a , private key of a second key pair for use in encrypting the second data")*

**and a second access right for a second user for the second data;**

*[Figure 5, ref. Num "100"; see the "encrypted document key" which is encrypted by the member's public key. Only the Member who has access to the information could use his corresponding private key to decrypt and get the document key which allows the member to access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key."];*

• **denies access to the second data, wherein the denying access comprises at least one of logging information regarding the denial of**

**access to the second data, and notifying security personnel regarding the denial of access to the second data [Column 16, lines 38-50]** (*"Accordingly, the collaborative access controller 44 performs a limiting step 156 to limit access to the information in the data portion 94 of the work group document 90. In one embodiment, the limiting step merely denies the user access by preventing decryption of the data portion 94. In other embodiments, decryption is prevented and additional steps are taken as well. One embodiment logs information about the failed attempt, such as the time, workstation, collaborative document name, user identifier, etc. Another embodiment uses e-mail, telephony, alarms, or other conventional means to notify security personnel of the failed attempt. A third embodiment both logs the information and notifies security."*)

**Carter** does not explicitly disclose

Wherein the document has the first data portion and a second data portion,  
receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right

However, in the same field of endeavor, **Rider** discloses,

**Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion,** [paragraph 0044, figure 4A & 0034-0035] (As

*shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is, **one or more access rights can be associated with portion 406**. Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)*

**Receiving a request from the user to access the document;  
comparing the request with the access right; and allowing access to  
only the first data portion in accordance with the access right**

[Paragraph 0034-0035 paragraph 0044, figure 4A] *(On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user **request to access one or more documents** as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource, **a particular document or only a portion of a document**. Furthermore on paragraph 0035, the following has been disclosed. “By restricting access in relation to a document’s content, a more fine-grained approach to configuring, managing and monitoring network resources is realized. Hence, tier two security restricts a user to data **constituting a portion of an entire document rather than***

***providing complete or no access to that document. For example, FIG. 4A depicts document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user.”)***

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion and receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right as per teachings of **Rider** into the method as taught by **Carter**, in order to provide a more fine-grained access control to the resources (portions of documents) [See *For instance Rider on paragraph 0035*].

17. **Independent claim 21 is rejected on the same reason as that of the above independent claim 11, However independent claim 21 further recites additional limitation. Thus the following rejection only considers the additional limitation.**

**As per independent claim 21 Carter discloses a method for controlling access to a document, [Abstract] comprising:**

- **Determining an access right for a user; (Column 12, lines 56-63; column 15, lines 62-67; abstract and column 8, lines 27-29)**

~~Access Control~~ Methods FIGS. 4-9 illustrate one method according to the present invention for controlling collaborative access to the work group document 90. In particular, the method includes computer-implemented steps for collaboratively encrypting the document 90 (FIG. 6) and steps for restricting access to the data portion 94 of the collaboratively encrypted document (FIG. 9)).

- **building a member definition** [Figure 5, see "member definition"] **comprising a member identifier** [Figure 5, ref. Num "98", See "member identifier"], **an access control** [See column 12, lines 56-57; column 13, lines 52-62, see figure 5, ref. Num 100, "encrypted document key" signed by the public key of the member. Only the member with the corresponding private key can access the document. In particular see the following which is disclosed on column 13, lines 64-column 14, lines 5, "The encrypted document key 100 is formed by encrypting the document key obtained during the step 110 with the public key of the member in question, which was obtained during the step 116. Note that the underlying document key is the same for each member of the collaborative group, but the encrypted form 100 of the document key is unique to each member. Those of skill in the art will appreciate. that the encrypted document key 100 can be decrypted only by using the private key 80 that corresponds to the public key 78 used to encrypt the document-key. "See also "collaborative access controller 44" which is described on column 6, lines 11-22 as the access controller which restrict access to the members only. Non members are restricted from accessing the information. See for instance the following

disclosed on column 6, lines 11-12, "users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot"] **and a private key of a key pair for enabling the first user to encrypt the document** [column 14 lines 16-22 and column 14, lines 4-5] ("As noted, the member definition 96 includes the encrypted message digest 102 if the member in question has collaboratively signed the document 90. As explained in greater detail below in connection with FIG. 10, the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and **then encrypting that message digest with the private key 80 of the member who is signing the document 90.**" Furthermore on column 14, lines 4-5, it has also been disclosed that the private key 80 is a key pair which corresponds to the public key 78. Thus, the message digest 102 which is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90 implicitly contains the private key of the member who is signing the document. With out the private key, it is not possible to produce the said message digest. Furthermore as it is disclosed on column 14, lines 4-5, the private key 80 is a key pair which corresponds to the public key 78 and this meets the argued limitation, "building a member definition comprising, a private key of a key pair for use in encrypting the document")

**and a digital signature.**[See also figure 5, ref. Num “102”, “encrypted message digest”, signed by the private key. In particular see what is disclosed on column 14, lines 15-21, “the encrypted message digest 102 is formed by generating a message digest based on the current contents of the data portion 94 of the document 90 and then encrypting that message digest with the private key 80 of the member who is signing the document 90.” See also the abstract and column 6, lines 11-12, “collaborative signatures, such that members of the group can digitally sign a particular version of the data portion. These collaborative signatures can then be used to advantage in ways similar to conventional individual digital signatures. For instance, the collaborative signatures can be used to identify the signing member.”] **and associating the member definition with the user.** [Figure 5 and column 6, lines 11-22, See “Users who are currently members of a collaborative group can readily access the information, while users who are not currently members of the group cannot”]

and

- **Linking the member definition to a portion of a document.**

[Figure 6, ref. Num “120”] (“Link member definition(s) with document.”)

**Carter** does not explicitly disclose

linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion,

receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right

However, in the same field of endeavor, **Rider** discloses,

**Linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion,** [paragraph 0044, figure 4A & 0034-0035] *(As shown, document 400 includes descriptor portion 402 and data portion 404. Descriptor portion 402 can include basic information about the device and its operation whereas data portion 404 can include actual data, which can be employed by specific applications. Portion 406 is a portion of data 404 that has its access governed in accordance with the principles of tier two security as described herein. That is, **one or more access rights can be associated with portion 406.** Although one portion 406 is shown, an ordinarily skilled artisan will appreciate that the same or other access rights can govern other portions of data portion 404.)*

**Receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right** [Paragraph 0034-0035 paragraph 0044, figure 4A] *(On paragraph 0034, the following has been disclose. Moreover, security manager 170 can permit, restrict or completely deny a user **request to access one or more documents** as well as the contents of those documents. A document or a portion thereof can represent a command for, or a configuration of, one of*



*devices 135 such as a router or switch. Security manager 170 governs by determining whether a particular user has access rights to a specific network resource, **a particular document or only a portion of a document. Furthermore on paragraph 0035, the following has been disclosed. "By restricting access in relation to a document's content, a more fine-grained approach to configuring, managing and monitoring network resources is realized. Hence, tier two security restricts a user to data constituting a portion of an entire document rather than providing complete or no access to that document. For example, FIG. 4A depicts document portion 406 that is accessible. Note that other portions of document 400 are not necessarily accessible to that user."***

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the feature such as linking the member definition to a first data portion of a document, wherein the document has the first data portion and a second data portion and receiving a request from the user to access the document; comparing the request with the access right; and allowing access to only the first data portion in accordance with the access right as per teachings of **Rider** into the method as taught by **Carter**, in order to provide a more fine-grained access control to the resources (portions of documents) [See For instance *Rider* on paragraph 0035]

18. **As per dependent claims 12-13 the combination of Carter and Rider**

discloses a method as applied to claims above. Furthermore, **Rider** discloses the method, wherein the access controller limits access to the

document in accordance with the first access right and the second access right. And, wherein the first user identifier and the second user identifier identify the same user and the first access right and the second access right identify different access rights [Paragraph 0034-0035 paragraph 0044, figure 4A].

19. **As per dependent claim 14 the combination of Carter and Rider**  
**discloses a method as applied to claims above. Furthermore, Carter discloses the method wherein the first member definition contains a digital signature.** *[Abstract and figure 10, ref. Num "184"]*
20. **As per dependent claim 15 the combination of Carter and Rider**  
**discloses a method as applied to claims above. Furthermore, Carter discloses the method wherein the first member definition and second member definition are stored remotely from the document.**  
*[column 14, lines 35-38]*
21. **As per claim dependent 16 the combination of Carter and Rider**  
**discloses a method as applied to claims above. Furthermore, Carter discloses the method where in the first and second the member definition are stored in the document.** *[Column 14, lines 31-34] ( "In one embodiment, linking is accomplished by **storing** the encrypted data portion 94 and the prefix portion 92 (including one or more **member definitions** 96) together in a file on a disk, tape, or other conventional **storage** medium.")*

**22. As per dependent claims 17-20 the combination of Carter and Rider**  
**discloses a method as applied to claims above. Furthermore, Carter**  
**discloses the method wherein the document is tagged**  
**document/XML document/text document/binary document [Column**  
**9, lines 32-61]**

### *Conclusion*

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

**A.** U.S Publication No. 2005/0021938 A1 to Kidokoro discloses the following. "If a link to a document is detected, each of the addresses identified in the e-mail message are extracted (step 206). The extraction of the addresses can also be performed by the e-mail server 20 or e-mail application used to create the e-mail message. The extracted addresses are then used to create a user account (step 208). The user account includes information identifying one or more users, such as by their addresses. The user account also includes information identifying what rights each user has to access a document, i.e., **an access control list to the document. The document being accessed can be a document stored in the file server 40. The user account can be stored in the user management database 30. The user account can be a single account storing information for each of the users addressed in the e-**

Art Unit: 2432

**mail message. This single account can be associated with a particular document and store information identifying access control information to the document for one or more users.”** [See at least paragraph 0022]

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system.

/Samson B Lemma/  
Examiner, Art Unit 2432